

# Claims

- [c1] A method for providing secure access to applications, the method comprising the steps of:  
receiving a request from a user to execute an application;  
determining a minimal set of computing privileges necessary for the user to use the requested application; and  
invoking an execution environment for the user having the determined set of privileges.
- [c2] The method of claim 1, comprising the further step of:  
returning an identifier for the execution environment to the requesting user.
- [c3] The method of claim 2, wherein the identifier is used to using the identifier and a remote presentation level protocol to connect the user to the execution environment.
- [c4] The method of claim 1 wherein step (a) comprises receiving an HTTP-based request from a user to execute an application.
- [c5] The method of claim 1 wherein step (b) comprises accessing a policy-based decision system to determine a minimal set of computing privileges necessary for the

user to use the requested application.

- [c6] The method of claim 1 wherein step (b) comprises analyzing requirements of an application to determine a minimal set of privileges necessary for the user to use the requested application.
- [c7] The method of claim 1 further comprising the step of receiving an indication of a dataset on which the application operates.
- [c8] The method of claim 5 wherein step (b) comprises accessing a confidentiality policy associated with the identified dataset to determine a minimal set of computing privileges necessary for the user to use the requested application.
- [c9] The method of claim 1 wherein step (b) further comprises determining a minimal set of computing privileges necessary for the user to use the requested application based, at least in part, on a role assigned to the user.
- [c10] The method of claim 1 wherein step (c) further comprises creating an execution environment for the user having the determined set of privileges.
- [c11] The method of claim 1 wherein step (c) further comprises identifying a previously-existing execution envi-

ronment for the user having the determined set of privileges.

[c12] The method of claim 1 further comprising the step of receiving from the user a request to execute a second application.

[c13] The method of claim 10 further comprising the steps of: determining a minimal set of computing privileges necessary for the user to use the second requested application; and  
invoking a second execution environment for the user having the second determined set of privileges.

[c14] The method of claim 1 further comprising the steps of initiating a connection with a client system associated with the user.

[c15] An application server system providing secure access to hosted applications, the system comprising:  
a policy based decision system receiving a request from a user to execute an application and determining a minimal set of privileges required by the user to execute the application; and  
an account administration service in communication with said policy based decision system, the account administration service invoking an execution environment for

the user having the determined set of privileges.

- [c16] The system of claim 15 further comprising a connection manager in communication with said policy based decision system, said connection manager receiving from a client system a request by the user to execute the application and transmitting to said policy based decision system an identification of said user and an identification of said application.
- [c17] The system of claim 16 wherein said connection manager communicates with the client using a presentation-level protocol.
- [c18] The system of claim 17 wherein said presentation-level protocol is selected from the group consisting of RDP, ICA, and X.
- [c19] The system of claim 15 wherein said connection manager transmits an identification of the user's role to said policy based decision system.
- [c20] The system of claim 15 wherein said policy-based decision system is based on a declared plurality of rules.
- [c21] The system of claim 15 wherein said policy-based decision system analyzes a set of requirements of the requested application to determine a minimal set of privi-

leges required by the user to execute the requested application.

[c22] The system of claim 15 wherein said connection manager receives an identification of a dataset that the application will process.

[c23] The system of claim 18 wherein said policy based decision system accesses a confidentiality policy associate with the identified dataset to determine a minimal set of privileges required by the user to execute the application.

[c24] The system of claim 15 wherein said account administration service creates an execution environment having the determined minimal set of privileges.

[c25] The system of claim 15 wherein said account administration service identifies a previously-existing execution environment having the determined minimal set of privileges.

[c26] An article of manufacture having embodied thereon computer-readable program means for providing secure access to applications, the article of manufacture comprising:

computer-readable program means for receiving a request from a user to execute an application;

computer-readable program means for determining a minimal set of computing privileges necessary for the user to use the requested application; and  
computer-readable program means for invoking an execution environment for the user having the determined set of privileges.

[c27] The article of manufacture of claim 27 further comprising computer-readable program means for accessing a policy-based decision system to determine a minimal set of computing privileges necessary for the user to use the requested application.

[c28] The article of manufacture of claim 27 further comprising computer-readable program means for determining a minimal set of computing privileges necessary for the user to use the requested application based, at least in part, on a role assigned to the user.

[c29] An application server system providing secure access to hosted applications, the system comprising:  
a policy based decision system receiving a request from a user to execute an application and determining a minimal set of privileges required by the user to execute the application;  
an account administration service in communication with said policy based decision system, the account adminis-

tration service invoking an execution environment for the user having the determined set of privileges; and a connection manager in communication with said policy based decision system, said connection manager receiving from a client system an RDP request by the user to execute the application and transmitting to said policy based decision system an identification of said user and an identification of said application.